

SECURE DIGITAL APPLIANCE AND METHOD FOR PROTECTING DIGITAL CONTENT

ABSTRACT OF THE DISCLOSURE

5 A method and apparatus for protecting digital content. A secure digital
appliance is disclosed for receiving communications coupled over a
communication network. A private key of a private key and public key pair is
stored in the secure digital appliance in such a way that the stored private key
cannot be obtained by tampering with the secure digital appliance. Upon
10 receipt of a session initiation message that is encrypted using the public key (of
the private key and public key pair) the secure digital appliance decrypts the
session initiation message using the stored private key to obtain a session key.
The session key is then used to decrypt communications that include encrypted
digital content. The secure digital appliance includes a local output device
15 (e.g., a TV screen and/or speakers) that is operable to provide protected output
of the digital content. The secure digital appliance does not contain any
provision for output other than the protected output of digital content. Because
the secure digital appliance does not allow for any output of the digital content
other than the protected output, the end user cannot obtain a high quality digital
20 copy of the digital content. Therefore, there is little chance that the security of
digital content will be compromised.